REMARKS

This communication is a full and timely response to the aforementioned final Office Action dated February 11, 2009. Claims 1-12, 17-20, 22-24, and 28-33, as presented in Amendment filed on December 29, 2009, are not amended and remain in the application. Thus, claims 1-12, 17-20, 22-24, and 28-33 are pending. Claims 1, 7, 17 and 31 are independent.

Reconsideration of the application and withdrawal of the rejections of the claims are respectfully requested in view of the foregoing amendments and the following remarks.

I. Rejections Under 35 U.S.C. § 112

A. Claims 31-33 were rejected under 35 U.S.C. § 112, first paragraph, as allegedly failing to comply with the written description requirement. This rejection is respectfully traversed.

Claim 31 recites "a computer-readable recording medium having a computer program recorded thereon for causing a computing device…to perform operations comprising…." In rejecting claim 31, the Office asserted that "a medium was not described in the original specification." This assertion is not supportable.

Contrary to the Office's assertion, the specification and drawings disclose several examples of computer-readable recording mediums. With reference to Figure 1, an exemplary embodiment provides a communication system in which a device 100 and a client 200 communicate data with each other through a network. According to an exemplary configuration as described in paragraph [0022] spanning pages 7 and 8 of the specification, the device 100 is encompassed by a printer or multifunctional peripheral (MFP), and the client 200 is encompassed by a personal computer (PC). As described in paragraph [0023] on page 8 of the specification, an MFP can function as a printer, a copying machine, a scanner and the like.

Figure 2 is a block diagram illustrating an exemplary configuration of structural components of the device 100 (e.g., printer, MFP). As described in paragraph [0023], for example, the device 100 includes, *inter alia*, a central processing unit (CPU) 110 connected through an internal bus 112 to a random access memory (RAM) 114, a read-only memory (ROM) 116, and a storage device 118 such as a

hard disk drive. The storage device 118 stores programs, such as a web server, a program 122 for creating a root certificate, and a program 124 for creating a self-made certificate (second certificate). In addition, paragraph [0025] on page 9 of the specification provides that programs and data can be stored in storage devices such as the hard disk in the storage device 118. Such programs and data can also be stored in a portable computer-readable recording mediums, such as a flexible disk or various optical disks (e.g., compact disk 226a illustrated in Figure 3). If such a computer-readable recording medium is utilized, the programs and data recorded thereon can be accessed by a drive (e.g., drive 226 illustrated in Figure 3).

To satisfy the written description requirement, a patent specification must describe the claimed invention in sufficient detail that one skilled in the art can reasonably conclude that the inventor had possession of the claimed invention. See MPEP 2163(I), second paragraph (citations omitted). It is well-settled that the subject matter of a claimed invention need be described literally in the specification (i.e., using the exact same terms or *in haec verba*). See MPEP 2163.02.

The Office appears to be improperly relying on an *in haec verba* standard for interpreting whether the specification and drawings provide a written description of a "computer-readable medium." In particular, the Office alleged that "a computer-readable medium" was not described in the original specification.

Contrary to the Office's unsupported assertion, the specification and drawings disclose numerous examples of computer-readable recording mediums, such as the components corresponding to reference numerals 114, 116, 118 in Figure 2, and the components corresponding reference numerals 204, 206, 214 and 226a in Figure 3, for example. Therefore, the specification and drawings unequivocally provide a written description of a "computer-readable recording medium," as recited in claims 31-33, in the form of several examples that one skilled in the art would readily interpret as a disclosure for a "computer-readable recording medium."

If the Office is to maintain an *in haec verba* interpretation of written description for terms recited in the claims, Applicant respectfully requests the Office to produce authoritative support for such an interpretation.

Furthermore, in rejecting claims 31-33 under 35 U.S.C. § 112, first paragraph, the Office asserts that "computer readable mediums, such as signals and waves, are directed toward non-statutory subject matter." Based on this statement, it appears that the Office is confusing the requirements for establishing a rejection under 35 U.S.C. § 112, first paragraph, and the requirements for establishing a rejection under 35 U.S.C. § 101.

As demonstrated above, the specification and drawings clearly satisfy the written description requirement of 35 U.S.C. § 112, first paragraph, by reasonably conveying to one skilled in the art that the inventors, at the time the application was filed, had possession of the inventions of claims 31-33.

Furthermore, it is noted that the Office disregarded the term "recording" in the recited "computer-readable recording medium" of claims 31-33. It is not clear whether the Office ignored this term in the Office Action in an attempt to justify the mosaic rejections of claims 31-33 on the basis of written description and non-statutory subject matter. All words in the claim must be considered when determining the scope of the claim. See, e.g., *Diamond v. Diehr*, 450 U.S. 175,188-189, 209 USPQ 1, 9 (1981); MPEP 2106(II)(C), twelfth paragraph; MPEP 2143.03.

A computer-readable recording medium cannot be reasonably interpreted as a signal or wave, because a signal or wave cannot record a computer program or data.

Moreover, by reciting the computer program as being recorded (encoded) on a computer-readable storage medium and executed by a computing device, the structural and functional interrelationships between the computer program, the computer-readable recording medium and the computing device permit the functionality of the computer program to be realized (see MPEP 2106.01(I), second paragraph). Therefore, claims 31-33 recite patentable subject matter under 35 U.S.C. § 101.

The Office also alleged that the subject matter of claim 33 is not supported in the specification. The rejection of claim 33 under 35 U.S.C. § 112, first paragraph, is respectfully traversed.

Claim 33 depends from claim 31, which recites the computing device as being configured to communicate with a client through a network to send information to the

client, which uses the information to communicate with the computing device. Claim 31 also recites that the information and a root certificate are sent to the client, before a request for communication is requested by the client.

Claim 33, in further defining the subject matter of claim 31, recites that the information is a printer driver. The Office asserted that the "specification does not teach sending a printer driver to a client before a request for communication is requested by the client." This assertion is not supportable.

The subject matter of claim 33 is supported throughout the specification and drawings. See, for example, paragraph [0026] spanning pages 9-11 of the specification. For instance, according to an exemplary embodiment, the root certificate 126 created by the device 100 has been installed in the client 200 before the client 200 requests to communicate with the device 100 according to a secured protocol (e.g., SSL). As described in lines 14-17 on page 10 of the specification, the root certificate 126 may be installed "when the printer driver 218 for the device 100 is installed in the client 200." As described in paragraph [0024] spanning pages 8 and 9 of the specification, the printer driver 218 generates print data to be send to a printer or MFP as one of the devices 100.

Consistent with the features recited in claims 31 and 33, paragraph [0028] spanning pages 11 and 12 provides, with reference to Figure 4, that when the client 200 request a secure connection to the device 100, the device 100 creates a second certificate (self-made certificate) and sends the second certificate to the client 200.

Thus, the specification clearly provides that a printer driver, as one type of information used by the client to communicate with the exemplary computing device 100, is sent with the root certificate to the client before a request for communication is requested by the client. Therefore, Applicant respectfully submits that the subject matter of claim 33 is clearly disclosed in the specification and drawings.

Accordingly, for at least the foregoing reasons, Applicant respectfully requests that the rejection of claims 31-33 under 35 U.S.C. § 112, first paragraph, be withdrawn as being improper.

B. Claim 32 was rejected under 35 U.S.C. § 112, second paragraph, as allegedly being indefinite. This rejection is respectfully traversed.

Claim 32 recites that "the computing device is a device which functions as a printer." The Office alleged that "it is unclear what functions of a printer the computing device may have." Furthermore, the Office alleged that "it is unclear whether the applicants are trying to limit the device to be a non-printing device which functions as a printer."

Applicant respectfully submits that these assertions are not supportable. As described above, the specification and drawings provide support for an embodiment in which the device 100 is a printer or MFP (see paragraphs [0022]-[0023] of the specification, for example). Therefore, Applicant cannot understand why claim 32 is believed to be indefinite, because the features of claim 32 are clear and particularly point out the claimed invention.

It appears that the Office is mistaking breadth for indefiniteness. It is well-settled that breadth of a claim is not to be equated with indefiniteness. *In re Miller*, 441 F.2d 689, 169 USPQ 597 (CCPA 1971); see MPEP 2173.04. If the scope of the subject matter embraced by the claims is clear, and if Applicant has not otherwise indicated that he intends the invention to be of a scope different from that defined in the claims, then the claims comply with 35 U.S.C. § 112, second paragraph.

Applicant respectfully submits that the features of claim 32 are clear. While it appears that the Office would prefer the scope of claim 32 to be narrower, the breadth of a claim is not the test for indefiniteness. Therefore, Applicant respectfully submit that the Office has mistakenly confused breadth for indefiniteness.

For instance, the Office poses the question of "what functions of a printer the computing device may have." There is no basis for this question. One skilled in the art understands that the term "printer" means a device which can form an image and/or textual characters onto a physical medium, such as paper. Accordingly, the recitation that "the computing device is a device which functions as a printer" is not indefinite.

Moreover, the Office's assertion that "it is unclear whether the applicants are trying to limit the device to be a non-printing device which functions as a printer" is similarly not supportable. There is no basis for this interpretation.

While the Office is afforded the broadest reasonable interpretation of a feature recited in a claim, the broadest reasonable interpretation of the claimed feature must be consistent with the interpretation that those skilled in the art would reach. See In re Cortright, 165 F.3d 1353, 1359, 49 USPQ2d 1464, 1468 (Fed. Cir. 1999); MPEP 2111. There is no feature recited in claim 32 which would provide any reasonable basis for the Office's assertion that Applicant is "trying to limit the device to be a non-printing device which functions as a printer." This interpretation is not consistent with the interpretation that those skilled in the art would reach. In particular, there is nothing explicitly or implicitly recited in claim 32 to justify the Office's assertion that the computing device is a device which is a non-printing device which somehow functions as a printer.

It is well-settled that the ordinary and customary meaning of a claim term is the meaning that the term would have to a person of ordinary skill in the art. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1313, 75 USPQ2d 1321, 1326 (Fed. Cir. 2005); MPEP 2111.01(III). In the absence of an express intent to impart a novel meaning to the claim terms, the words are presumed to take on the ordinary and customary meanings attributed to them by those of ordinary skill in the art. *See, e.g., Brookhill-Wilk 1, LLC v. Intuitive Surgical, Inc.*, 334 F.3d 1294, 1298, 67 USPQ2d 1132, 1136 (Fed. Cir. 2003); *Toro Co. v. White Consol. Indus., Inc.*, 199 F.3d 1295, 1299, 53 USPQ2d 1065, 1067 (Fed. Cir. 1999).

Applicant has not attempted to impart a novel meaning to the term "device" so that it means "a non-printing device with functions [of] a printer." The terms of claim 32 are to be given their ordinary and customary meaning.

Accordingly, for at least the foregoing reasons, Applicant respectfully requests that the rejection of claim 32 under 35 U.S.C. § 112, second paragraph, be withdrawn, since the Office is improperly equating breadth for indefiniteness and improperly employing an interpretation contrary to the interpretation that one skilled in the art would reach.

II. Rejections Under 35 U.S.C. § 103

Claims 1, 4, 5, 7, 10, 12, 17, 20, 22-24, and 30 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Smetters (U.S. Patent Application Publication

No. 2004/0088548, hereinafter "Smetters") in view of Benussi et al. (U.S. Patent Application Publication No. 2001/0044898, hereinafter "Benussi").

(1) Independent Claims 1, 7, 17 and 31

Claim 1 recites a communication system in which a device and a client communicate data with each other through a network. Claim 1 recites that the device comprises a first storage device which stores a root certificate including a public key paired with a private key and signed with the private key. In addition, claim 1 recites that the device comprises a certificate creator which creates, when a connection for communication is requested by the client, a second certificate designating the root certificate as a certificate authority at a higher level and being signed with the private key used to sign the root certificate.

Claim 7 recites a communication method for a communication system in which a device and a client communicate date with each other through a network, wherein the device holds a root certificate including a public key paired with a private key and being signed with the private key. In addition, the method of claim 7 includes the device creating, when a connection for communication is requested by the client, a second certificate designating the root certificate as a certificate authority at a higher level and being singed with the private key used to sign the root certificate when data is sent to the client.

Claim 17 recites a device to be used in a communication system in which the device and a client communicate with each other through a network, the device sends information to the client, and the client uses the information to communicate with the device. The device of claim 17 comprises a first storage device which stores a pair of a public key and a private key, and a second storage device which stores a root certificate signed with the private key. In addition, the device of claim 17 comprises a certificate creator which creates, when a connection for communication is requested by the client, a second certificate designating the root certificate as a certificate authority at a higher level and being signed with the private key used to the sign the root certificate.

Claim 31 recites a computer-readable recording medium having a computer program recorded thereon that causes a computing device to perform operations of

storing a pair of a public key and a private key, storing a root certificate signed with the private key, and sending information and the root certificate including the public key to the client, before a request for communication is requested by the client. In addition, claim 31 recites that the computer program causes the computing device to perform an operation of creating, when the connection for communication is requested by the client, a second certificate designating the root certificate as a certificate authority at a higher level and being signed with the private key used to sign the root certificate.

Accordingly, independent claims 1, 7, 17 and 31 each recite that the device creates a second certificate, which designates the root certificate as a certificate authority at a higher level, where the second certificate is signed with the private key used to sign the root certificate, when a connection for communication is requested by the client.

Applicant respectfully submits that the applied references do not disclose or suggest the above-described features of independent claims 1, 7, 17 and 31 for at least the following reasons.

The Office asserted that the feature of a second certificate, which designates a root certificate as a certificate authority at a higher level, and which is signed with a private key is somehow disclosed in Smetters. This assertion is contrary to the *actual* disclosure of Smetters. In striving to arrive at the subject matter of claims 1, 7, 17 and 31, the Office mischaracterized the disclosure of Smetter as disclosing something it does not. In particular, the Office asserted that it can selectively apply the disclosure of paragraphs [0025] and [0031] and intentionally disregard the disclosure of other portions of Smetters, since this method of interpretation is believed to permit the Office to arrive at the subject matter of the claimed invention.

The Office's interpretation of Smetters to arrive at the subject matter of the claimed invention is analogous to referring to the beginning stage of a process, mischaracterizing the final stage of the process to meet its erroneous interpretation, and skipping over every intermediate stage because each intermediate stage, if considered objectively, refutes the Office's characterization of the outcome from the final stage in the process. However, in following this improper methodology to support its improper interpretation of Smetters, the Office ignored portions of

Smetters which unmistakably refute the Office's allegation of what Smetters discloses. Furthermore, in following this improper methodology, the Office is also impermissibly ignoring well-settled principles of examination.

A reference must be considered in its entirety, i.e., as a whole, including portions that would teach away from the claimed invention. *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 220 UPSQ 303 (Fed Cir. 1983); MPEP 2141.03.VI.

Smetters discloses an opposite configuration to that of claims 1, 7, 17 and 31. The Office alleges that Smetters disclose a technique of signing a second certificate with the same private key used to sign the root certificate. The *actual* disclosure of Smetters refutes this assertion. In striving to arrive at the subject matter of claims 1, 7, 17 and 31, the Office disregarded the intermediate steps of Smetters that occur between (A) the first device 12(1) generating a root certificate 30 (paragraph [0025] of Smetters) and (B) the first device 12(1) generating and sending a second certificate 40, together with the root certificate 30, to the second device 12(2) (paragraph [0031]). Smetters discloses two different techniques of transitioning from point (A) to point (B). In particular, Smetters discloses that (1) the first laptop 12(1) signs the second certificate 40 with the public key that is generated by the first device 12(1), or the first device 12(1) signs the second certificate 40 with the public key that is transmitted to the first device 12(1) by the second device 12(2). In either case, the first device 12(1) signs the second certificate 40 with a public key.

In view of the Office's misrepresentation of the disclosure of Smetters in striving to arrive at the subject matter of claims 1, 7, 17 and 31, the *actual disclosure* of Smetters is summarized below to illustrate how the *actual disclosure* of Smetters refutes the Office's interpretation. The two different techniques of transitioning from point (A) and point (B) are also discussed below, even though the Office believes it can disregard them.

(1) Generation of Root Certificate 30

Smetters discloses a system 10 for creating a shared resource space 20 containing resources 22, 24 to be shared among a first device 12(1) and a second device 12(2) (see Figures 1 and 3). The first device 12(1), which has access to the resources 22, 24, generates a root key pair to be used for authentication and

encryption when providing the device 12(2) with access to the shared space 20 (see paragraph [0025], step 100 in Figure 2, and step 120 in Figure 4). In order to share access to the space 20, the first device 12(1) then "generates a root certificate 30 for the new space 20, and digitally signs the [root] certificate 30" (see paragraph [0025], step 100 in Figure 2, and step 130 in Figure 4) (emphasis added).

(2) Establishing Secure Communication

After the first device 12(1) has generated the root certificate 30, the first device 12(1) then transmits range-limited signals to the second device 12(2) to establish a secure communication channel between each other (see paragraph [0028], step 200 in Figure 2). Paragraph [0028] of Smetters also discloses that the second device 12(2) may initially send the range-limited signals to initiate the establishment of a secure communication channel with the first device 12(1). Smetters discloses that the range-limited signal transmitted from the first device 12(1) includes a public key to secure the communication channel between the first and second devices 12(1), 12(2) (see paragraph [0029]). Once a secure communication channel between the first device 12(1) and second device 12(2) has been established, Smetters discloses that the first device 12(1) then sends an invitation message to the second device 12(2) that invites the second device 12(2) to accept access to the shared space 20 (see paragraph [0030], and step 300 in Figure 2).

(3) Decision by Second Device 12(2) Concerning Which Public Key to Use

Smetters discloses that the second device 12(2) then decides whether to use a particular public key (i.e., the public key included in the range-limited signal from the first device 12(1) or a public key generated by the second device 12(2)) to communicate with the first device 12(1) (see paragraph [0032] and step 510 in Figure 6). The two different techniques are discussed in sections 3A and 3B below.

(3A) Second Device 12(2) Decides to Use Other Public Key

If the second device 12(2) decides to use a particular public key instead of the public key included in the range-limited signal (section (2) above) from the first

device 12(1), the second device 12(2) transmits the desired public key to the first device 12(1) (see paragraph [0032] and step 520 in Figure 6). If the second device 12(2) decides to use a particular public key for encryption instead of the public key generated by the first device 12(1), it is not necessary for the first device 12(1) to transmit the corresponding private key to the second device 12(2), because the corresponding private key 12(2) is already in the possession of the second device 12(2).

(3B) Second Device 12(2) Decides to Use Public Key Generated By First Device 12(1)

On the other hand, if the second device 12(2) decides to use the public key generated by the first device 12(1) and included in the range-limited signal, the first device 12(1) generates a pair of a public key and a private key, and sends the private key of the generated key pair to the second device 12(2) (see paragraph [0033], and steps 530 and 540 in Figure 6). If the second device 12(2) desires to use the public key generated by the first device 12(1), the first device 12(1) must therefore send the corresponding private key to the second device 12(2), or else the second device 12(2) could not decrypt a communication that was encrypted with the public key generated by the first device 12(1).

It is noted that in lines 2-3 on page 3 of the Office Action, the Office asserted that "sending private keys [is] contrary to the principles of cryptography." As discussed above, paragraph [0033] of Smetters specifically refutes this assertion. Perhaps the Office is substituting its view of how cryptography should ideally operate for the *actual* disclosure of Smetters.

(4) Generation of Second Certificate 40

After the second device 12(2) decides which public key to use (3(A) or 3(B)), the first device 12(1) then creates a second certificate 40 using either the public key sent from the second device 12(2) or the public key of the key pair generated by the first device 12(1) (see paragraph [0034], step 500 in Figure 2, and step 550 in Figure 6). The second certificate 40 designates the second device 12(2) as a member of the shared space 20 (see paragraphs [0031] and [0034], step 500 in Figure 2, and

step 550 in Figure 6). Smetters discloses that the first device 12(1) sends both the root certificate 30 and the second certificate 40 to the second device 12(2) at the same time as a certificate chain (see paragraph [0035]).

The different techniques used to generate the second certificate respectively correspond to whether (3A) the second device 12(2) decides to use a different public key, or (3B) the second device 12(1) decides to use the public key generated by the first device 12(1). The two different techniques of Smetters are disclosed in sections 4A and 4B below.

(4A) First Device Signs Second Certificate 40 With Public Key Sent By Second Device 12(2)

This technique of Smetters is illustrated in Figure 6 with respect to step 520. In this technique (4A), the second device 12(2) retains the private key corresponding to the public key transmitted to the first device 12(1), because the first device 12(1) signs the second certificate 40 with the public key and the second device 12(2) must therefore possess the corresponding private key in order to decrypt the second certificate 40. In public-private key cryptography, encrypted data can only be decrypted by using one key of a key pair, when the other key of the key pair was used to encrypt the key pair. Therefore, in view of the disclosure of Smetters that the second device 12(2) sends the public key to be used in signing the second certificate 40 to the first device 12(1), the second device 12(2) must retain possession of the corresponding private key in order to decrypt the second certificate 40 sent from the first device 12(1).

Furthermore, Applicant respectfully submits that it is not possible for the first device 12(1) to sign the second certificate 40 with a private key corresponding to the public key transmitted from the second device 12(2), because Smetters does not disclose or suggest that the second device 12(2) transmits the private key corresponding to the public key that was transmitted from the second device 12(2). Moreover, such an interpretation would be contradictory to the principles of public-private key cryptography.

Therefore, according to the first technique (4A) in which the second device 12(2) transmits a public key to the first device 12(1) and the first device 12(1) signs

the second certificate 40 with the public key received from the second device 12(2), the first device 12(1) does not sign the second certificate 40 with a private key corresponding to the public key transmitted from the second device 12(2).

Furthermore, the first device 12(1) does not sign the second certificate 40 with the private key used to sign the root certificate 30. Such a construction would not be possible according to the first technique (4A) of Smetters, because the root certificate 30 is generated by the first device 12(1) after the first device 12(1) has generated a root key pair (see paragraph [0025]), and the second certificate 40 is generated by the first device 12(1) using the public key transmitted from the second device 12(2). A public or private key of one root key pair does not correspond to a public or private key of another root key pair. Accordingly, it would not be possible according to the first technique (4A) of Smetters for the first device 12(1) to sign the second certificate 40 using the same private key used to sign the root certificate 30, because different key pairs are used for generating the root certificate 30 and the second certificate 40.

(4B) First Device 12(1) Signs Second Certificate 40 With Public Key Generated By First Device 12(1)

The second technique of Smetters is illustrated in Figure 6 with respect to steps 530 and 540. In this technique, the first device 12(1) generates a public and private key pair (step 530), and sends the private key corresponding to the public key pair to the second device 12(2) (see paragraph [0033]). The first device 12(1) must send the private key corresponding to the public key that is used to sign the second certificate 40, because the second device 12(2) would not be able to decrypt the second certificate 40 unless it was provided with the private key. The disclosure in paragraph [0033] further emphasizes that the first device 12(1) does not sign the second certificate 40 with the private key corresponding to the public key, because sending the private key of the newly generated key pair to the second device 12(2) would not, in any way, permit the second device 12(2) to decrypt the second certificate 40, if the second certificate 40 was hypothetically signed with the private key of the newly generated key pair. If the second certificate 40 was hypothetically signed with the private key of the newly generated key pair, then the first device

12(1) would need to send the public key of the newly generated key pair, so that the second device 12(2) could decrypt the second certificate 40. However, Smetters discloses the opposite technique in which the first device 12(1) transmits the private key to the second device 12(2), because the second certificate 40 is signed with the public key of the key pair that is newly generated by the first device 12(1).

Therefore, according to the second technique (4B) of Smetters in which the first device 12(1) generates a new key pair and transmits the private key of the newly generated key pair to the second device 12(2), Smetters does not disclose or suggest that the second certificate 40 is signed with a private key.

Furthermore, the first device 12(1) does not sign the second certificate 40 with the private key used to sign the root certificate 30. Such a construction is contradictory to the disclosure of Smetters. In particular, Smetters discloses that when the second device 12(2) elects to have the first device 12(1) use a public key generated by the first device 12(1) to generate the second certificate 40, the first device 12(1) generates a new key pair (see paragraph [0033, and step 530 in Figure 6]). The new key pair generated by the first device 12(1) to generate the second certificate 40 in step 530 of Figure 6 (corresponding to step 500 in Figure 2) is different from the key pair generated by the first device 12(1) to generate the root certificate 30 in step 120 of Figure 4 (corresponding to step 100 in Figure 2), because these key pairs are generated at different stages within the resource management process of Figure 2 and therefore are different key pairs. A public or private key of one root key pair does not correspond to a public or private key of another root key pair. Consequently, Smetters does not disclose or suggest that the first device 12(1) signs the second certificate 40 with the private key used to sign the root certificate 30.

Accordingly, for at least the foregoing reasons, Applicant respectfully submits that no disclosure of Smetters, even given the broadest reasonable interpretation, supports the Office's assertion that Smetters somehow discloses that the second certificate 40 is signed with a private key used to sign the root certificate. The Office's assertion is factually erroneous and is specifically refuted by the disclosure of Smetters.

Therefore, Applicant respectfully submits that that Smetters does not disclose or suggest that the second certificate 40 (or any other subordinate member certificate) is signed with the private key used to sign the root certificate 30.

Consequently, Smetters does not disclose or suggest that the device creates a second certificate, which designates the root certificate as a certificate authority at a higher level, where the second certificate is signed with the private key used to sign the root certificate, when a connection for communication is requested by the client, as recited in claims 1, 7, 17 and 31.

Benussi also does not disclose or suggest these features of claims 1, 7, 17 and 31. On the contrary, Benussi discloses that a root certificate ("Root CA") of a CSS (communication service system) 20 is signed with a private key of the CSS 20, and the root certificate of CSS 20 is pre-installed in the CB (connectivity box) 11 for the initial configuration of the CB 11 (see paragraph [0214], lines 24-30 and 51-55, and Figure 1).

However, similar to Smetters, Benussi does not disclose or suggest that a second certificate, which designates the Root CA of the CSS 20 as a certificate authority at a higher level, is signed with the private key of the CSS 20 used to sign the Root CA.

Therefore, neither Smetters nor Benussi disclose or suggest that the device creates a second certificate, which designates the root certificate as a certificate authority at a higher level, where the second certificate is signed with the private key used to sign the root certificate, when a connection for communication is requested by the client, as recited in claims 1, 7, 17 and 31.

Accordingly, for at least the foregoing reasons, Applicant respectfully submits that Smetters and Benussi, either individually or in combination, do not disclose or suggest all the recited features of claims 1, 7, 17 and 31.

Therefore, Applicant respectfully submits that claims 1, 7, 17 and 31 are patentable over Smetters and Benussi, since Smetters and Benussi, either individually or in combination, fail to disclose or suggest all the recited features of claims 1, 7, 17 and 31.

Furthermore, Applicant respectfully submits that the Office's proposed combination of Smetters and Benussi in an attempt to arrive at the subject matter of the claimed invention is not supportable.

It is well-settled that if a modification of an applied reference would change the principle of operation of the reference being modified, then there is no reason, suggestion or motivation to modify the reference in that manner. See In re Ratti, 123 USPQ 349 (CCPA 1959); MPEP 2143.01.VI.

However, in the present instance, the Office is proposing to change the principle of operation of Smetters in an attempt to arrive at the subject matter of the claimed invention. In particular, a major emphasis of Smetters is for the first device 12(1) to transmit both the root certificate 30 and the second certificate 40 at the same time, and the second device 12(2) stores the simultaneously received root and second certificates 30 and 40 together as a "certificate chain" (see paragraph [0305] and step 600 in Figure 2). As disclosed in paragraph [0305], the second device 12(2) uses the certificate chain to prove to other members of the shared space 20 that the second device 12(2) is authorized to access the shared space 20.

In contrast to the well-settled provisions of the impermissibility of changing the principle of operation of an applied reference, the Office proposed, on page 4 of the Office Action, that it would have been obvious to modify Smetters "to have stored the root certificate earlier." However, such a modification changes a principle of operation of Smetters, and therefore is not supportable.

Therefore, in addition to Smetters and Benussi failing to disclose or suggest all the recited features of claims 1, 7, 17 and 31, Applicant respectfully submits that the proposed combination of Smetters and Benussi is not supportable.

(2) Dependent Claims

Dependent claims 4, 5, 10, 12, 20, 22-24, 28-30, 32 and 33 recite further distinguishing features over Smetters and Benussi.

For example, claim 10 recites that, in the method of claim 7, when the client installs the root certificate, the installation is performed after the root certificate is confirmed by a user. In an attempt to arrive at the features of claim 10, the Office referred to paragraph [0031] of Smetters, which discloses that the operator of the

second device 12(2) decides whether to respond to the invitation from the first device 12(1) to gain access to the shared space 20. This does not amount to the features recited in claim 10, because Smetters does not disclose, suggest or contemplate that the operator of the second device 12(2) confirms the root certificate 30 prior to its installation. On the contrary, paragraph [0031] of Smetters merely discloses that the operator 12(2) decides whether he or she wants to gain access to the shared space 20, in response to the invitation message transmitted from the first device 12(1).

Claim 20 recites that the root certificate stored in the first storage device is stored in the second storage device prior to the transmission of the second certificate from the communication device. Claim 23 recites that, in the method of claim 7, the device sends the second certificate to the client after the root certificate is installed in the client.

As discussed above, a major emphasis of Smetters is for the first device 12(1) to send both the root certificate 30 and the second certificate 40 to the second device 12(2) at the same time, and for the second device 12(2) to store the received certificate chain so as to be able to prove that it has access to the shared resource space. Accordingly, Smetters discloses an opposite technique to the features of claims 20 and 23.

In an attempt to cure the deficiencies of Smetters, the Office has improperly changed a principle of operation of Smetters by applying Benussi. The improper combination of Smetters and Benussi is contrary to well-settled provisions, and therefore, Applicant respectfully submits that the combination of Smetters and Benussi to arrive at the features of claims 20 and 23 is not supportable.

Claim 22 recites that the verifier of the client is operable to verify the signature of the second certificate by decrypting the public key of the root certificate stored in the second storage device to obtain a first hash value, calculating a second hash value of the second certificate received from the device, and comparing the first and second hash values to determine if they are equal to each other.

The Office asserted that the features recited in claim 22 are disclosed in paragraphs [0041] and [0042] of Smetters. This assertion is not supportable. Paragraphs [0041] and [0042] of Smetters do not disclose or suggest the calculation of the first and second hash values and the subsequent comparison of the first and

second hash values, as recited in claim 22. Paragraphs [0041] and [0042] do not disclose or suggest the generation of hash values from either the root certificate 30 or the second certificate 40.

Claims 28 and 29 recite that the client stores the public key of the installed root certificate, prior to the client requesting the connection for communication to the device, and that the client verifies the signature of the second certificate received from the device by decrypting the second certificate with the public key of the root certificate stored in the client.

Smetters and Benussi do not disclose or suggest the features of claims 28 and 29. In particular, as discussed above, Smetters discloses that the second device 12(1) decrypts the second certificate 40 by using the private key that is either sent from the first device 12(1) (when the first device 12(1) generates a new key pair for the second certificate 40) or is already installed in the second device 12(2) (when the second device 12(2) transmits the public key for creation of the second certificate 40). Accordingly, Smetters does not disclose or suggest that the second device 12(2) verifies the signature of the second certificate 40 by decrypting the second certificate 40 with the public key of the root certificate 30.

Furthermore, Benussi does not disclose or suggest any second certificate corresponding to the claimed invention. Therefore, Applicant respectfully submits that claims 28 and 29 recite further distinguishing features over the applied references.

For at least the foregoing reasons, Applicant respectfully submits that Smetters and Benussi, either individually or in combination, do not disclose or suggest the features of dependent claims 10, 20, 22, 23, 28 and 29, in addition to failing to disclose or suggest all the recited features of claims 1, 7, 17 and 31.

Therefore, in addition to the patentability of claims 1, 7, 17 and 31 demonstrated above, Applicant respectfully submits that claims 10, 20, 22, 23, 28 and 29 recite further distinguishing features over Smetters and Benussi.

B. Claims 28, 29 and 31 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Smetters in view of Benussi and further in view of Schneier's Applied Cryptography, 2nd Edition (hereinafter "Schneier").

As demonstrated above, neither Smetters nor Benussi disclose or suggest that a device creates a second certificate, which designates the root certificate as a certificate authority at a higher level, where the second certificate is signed with the private key used to sign the root certificate, when a connection for communication is requested by a client, as recited in claims 1, 7, 17 and 31.

Similarly, Schneier also fails to disclose or suggest this feature of claims 1, 7, 17 and 31. Therefore, Schneier cannot cure the deficiencies of Smetters and Benussi. Consequently, no obvious combination of Smetters, Benussi and Schneier would arrive at the subject matter of claims 1, 7, 17 and 31, since Smetters, Benussi and Schneier, either individually or in combination, fail to disclose or suggest all the recited features of claims 1, 7, 17 and 31.

Therefore, Applicants respectfully submit that claims 1, 7, 17 and 31 are patentable over Smetters, Benussi and Schneier.

C. Dependent claims 2, 3, 6, 8, 9, 11, 18, 19, 26, 27, 32 and 33 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Smetters in view of Benussi and further in view of one or more of Schneier, Frailong et al. (U.S. Patent No. 6,012,100, hereinafter "Frailong'), Debry (U.S. Patent No. 6,918,042, hereinafter "Debry"), Slick (U.S. Patent Application Publication No. 2004/0109568, hereinafter "Slick"), and Vogel et al. (U.S. Patent No. 6,816,900, hereinafter "Vogel").

As demonstrated above, Smetters and Benussi each do not disclose or suggest a device that creates a second certificate, which designates the root certificate as a certificate authority at a higher level, where the second certificate is signed with the private key used to sign the root certificate, when a connection for communication is requested by the client, as recited in claims 1, 7, 17 and 31.

Similarly, Schneier, Frailong, Debry, Slick and Vogel also each fail to disclose or suggest these features of claims 1, 7, 17 and 31. Therefore, Schneier, Frailong, Debry, Slick and Vogel cannot cure the deficiencies of Smetters and Benussi for failing to disclose or suggest all the recited features of claims 1, 7, 17 and 31, since

the applied references, either individually or in combination, do not disclose or suggest all the recited features of claims 1, 7, 17 and 31.

Therefore, no obvious combination of Smetters, Benussi, Schneier, Frailong, Debry, Slick and Vogel would arrive at the subject matter of the claimed invention, since the applied references, either individually or in combination, fail to disclose or suggest all the recited features of at least claims 1, 7, 17 and 31.

Accordingly, for at least the foregoing reasons, Applicant respectfully submits that claims 1, 7, 17 and 31, as well as claims 2-6, 8-12, 18-20, 22-24, 28-30, 32 and 33 which depend therefrom, are patentable over the applied references.

The foregoing explanation of the patentability of independent claims 1, 7, 17 and 31 is sufficiently clear such that it is believed to be unnecessary to separately demonstrate the patentability of the dependent claims not specifically addressed above at this time. However, Applicant reserves the right to do should it become appropriate.

III. Conclusion

In view of the foregoing amendments and remarks, it is respectfully submitted that the present application is clearly in condition for allowance. Accordingly, a favorable examination and consideration of the instant application are respectfully requested.

If, after reviewing this Amendment, the Examiner believes there are any issues remaining which must be resolved before the application can be passed to issue, the Examiner is respectfully requested to contact the undersigned by telephone in order to resolve such issues.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: August 3, 2009

By: /Jonathan R. Bowser/
Jonathan R. Bowser
Registration No. 54574

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620